Physical Architecture Diagram

Overview

The Physical Architecture Diagram for Grow Management Consultants provides a detailed representation of the specific technologies and implementations that will be used to secure the organization's information assets, systems, and infrastructure across its head office and two new capital city offices. This diagram translates the conceptual security architecture into concrete physical components and their relationships.

Physical Architecture Components

Office Locations

Head Office

The head office implements the following security components:

1. **Network Security**:
2. Cisco Firepower Next-Generation Firewall (NGFW) for advanced threat protection
3. Cisco Identity Services Engine (ISE) for network access control
4. VPN Gateway for secure remote access
5. **Data Security**:
6. File server encryption for protecting data at rest
7. Data Loss Prevention (DLP) solution to prevent unauthorized data exfiltration
8. Database encryption for protecting sensitive database content
9. **Physical Security**:
10. Access control system for building and sensitive area access
11. CCTV surveillance for monitoring and recording physical activities
12. **Endpoint Security**:
13. Endpoint Detection and Response (EDR) solution for advanced threat detection
14. Disk encryption for protecting data on endpoints

Capital City Office 1

The first capital city office implements the following security components:

1. **Network Security**:
2. Cisco Firepower Next-Generation Firewall (NGFW) for advanced threat protection
3. Cisco Identity Services Engine (ISE) for network access control
4. SD-WAN for secure and optimized connectivity to head office
5. **Physical Security**:
6. Access control system for building and sensitive area access
7. CCTV surveillance for monitoring and recording physical activities
8. Alarm system for intrusion detection
9. **Endpoint Security**:
10. EDR solution and anti-malware for threat protection
11. Disk encryption and device controls for data protection

Capital City Office 2

The second capital city office implements the following security components:

1. **Network Security**:
2. Cisco Firepower Next-Generation Firewall (NGFW) for advanced threat protection
3. Cisco Identity Services Engine (ISE) for network access control
4. SD-WAN for secure and optimized connectivity to head office
5. **Physical Security**:
6. Access control system for building and sensitive area access
7. CCTV surveillance for monitoring and recording physical activities
8. **Endpoint Security**:
9. EDR solution for advanced threat detection
10. Anti-malware for malicious code protection

Cloud Services

The organization leverages cloud services with the following security components:

1. **Identity and Access Management**:
2. Azure AD / Microsoft Entra ID for centralized identity management
3. Multi-Factor Authentication for enhanced authentication security
4. **Data Protection**:
5. OneDrive encryption for protecting cloud-stored data
6. SharePoint security features for protecting collaborative content
7. **Application Security**:
8. Office 365 security features for protecting productivity applications
9. Cloud App Security for monitoring and controlling cloud application usage
10. **Threat Protection**:
11. Microsoft Defender for Cloud for cloud workload protection
12. Advanced Threat Protection for detecting and responding to sophisticated threats

Security Operations Center

The Security Operations Center (SOC) provides centralized security monitoring and management with the following components:

1. **Security Monitoring**:
2. Security Information and Event Management (SIEM) solution for log collection and correlation
3. Log collection and analysis for detecting security events
4. **Vulnerability Management**:
5. Vulnerability scanner for identifying security weaknesses
6. Patch management system for addressing vulnerabilities
7. **Incident Response**:
8. Incident Response platform for managing security incidents
9. Forensics tools for investigating security breaches

Connectivity and Integration

The physical architecture includes the following connectivity and integration components:

1. **Secure WAN Connections**:
2. Encrypted connections between the head office and capital city offices
3. SD-WAN technology for optimized and secure connectivity
4. **Secure Cloud Connectivity**:
5. Encrypted connections from all offices to cloud services
6. Centralized management of cloud security
7. **Security Monitoring and Management**:
8. Integration of all security components with the Security Operations Center
9. Centralized visibility and control of the security posture

Multilevel Security Implementation

The physical architecture implements a multilevel security model with:

1. **Role-Based Access Control with Least Privilege**:
2. Azure AD / Microsoft Entra ID for identity management
3. Cisco ISE for network access control
4. Application-level access controls
5. **Data Encryption**:
6. Encryption for data at rest (file servers, databases, endpoints)
7. Encryption for data in transit (VPN, TLS, secure communications)
8. Cloud data encryption (OneDrive, SharePoint)
9. **Defense in Depth**:
10. Multiple security layers at each location
11. Complementary security controls across network, application, data, and endpoint layers
12. Centralized monitoring and management

This physical architecture provides a comprehensive security implementation that addresses Grow Management Consultants' security requirements and supports its business objectives as it expands to new locations.